

Important Lessons Derived from X.500 Case Studies

D W Chadwick, University of Salford, Salford, M5 4WT

Abstract

X.500 is a new and complex electronic directory technology, whose basic specification was first published as an international standard in 1988, with an enhanced revision in 1993. The technology is still unproven in many organisations. This paper presents case studies of 15 pioneering pilot and operational X.500 based directory services. The paper provides valuable insights into how organisations are coming to understand this new technology, are using X.500 for both traditional and novel directory based services, and consequently are deriving benefits from it. Important lessons that have been learnt by these X.500 pioneers are presented here, so that future organisations can benefit from their experiences. Factors critical to the success of implementing X.500 in an organisation are derived from the studies.

Keywords: X.500, case study, directory service, X.400, electronic mail, critical success factors.

CONTENTS

1 Introduction	1
2 Background.....	2
3 The Survey.....	3
4 Important Lessons Learnt from the Case Studies	4
5 The Case Studies.....	14
6 Conclusion	23
7 Acknowledgments.....	24
8 Glossary of Terms	25
9 References.....	25
Appendix 1 Questionnaire for Providers of the X.500 Service.....	27

1 Introduction

X.500 is a new and complex electronic directory technology, whose basic specification was first published as an international standard by ISO and ITU-T (then the CCITT) in 1988 [16]. A revision of the standard which added replication and access control functionality was released in 1993 [17]. A general introduction to X.500 can be found in texts such as [11-14],

while a comprehensive description of the specification can be found in [15].

The technology is still unproven in many organisations. This set of case studies, believed to be the first of its kind, should provide valuable insights into how organisations are coming to understand this new technology, and are deriving benefits from it. Important lessons that have been learnt by these X.500 pioneers are presented here, so that future organisations can benefit from their experiences. Factors critical to the success of implementing X.500 in an organisation are derived from the studies.

2 Background

Early experimentation with X.500 services (1989 - 92) lay almost entirely within the academic and research environments. For example, in the UK, a handful of universities were given the Quipu [2] X.500 implementation and a Sun workstation and asked to start a pilot service. Similarly, in the US 15 East Coast Universities and research establishments started the White Pages pilot [3] in 1989. More recently (1992 onwards) government departments, their agencies and related organisations have become involved with X.500 services. For example, the Ministry of Agriculture and Fisheries in the UK and NASA in the US both have operational X.500 services. As yet very few commercial organisations have dipped their toes in the X.500 waters, and those that have are very reluctant to publish their results. Two notable exceptions to this are Digital and Control Data Systems, who now have fully operational X.500 services within their organisations. However, as these two companies are both suppliers of X.500 software, they obviously have a vested interest in proving the viability of X.500 technology. Data from other commercial organisations is hard to come by. Whilst a number of organisations e.g. BASF in Germany, Union Bank of Switzerland and City Bank in New York, are known to have experimented with X.500 technology, it has not proved possible to obtain information from them for this survey. Public utilities and services are also experimenting with X.500, for example the Southern Company in the US, the National Health Service in the UK and Electricity de France have all mounted pilot projects, and they are represented in this survey, but these organisations have not yet made the transition to full production services.

By far the largest body of available information comes from the university and research sector, and a number of these have responded to the survey. All of their early experiences are based on using variations of the Quipu software, which was both a publicly, and the first, available implementation of X.500. Quipu subsequently formed the basis of a number of commercial products from suppliers such as Control Data Systems, Nexor and the ISODE Consortium. In the case studies that follow, it is interesting to note that only three of the respondents (Digital, UK MoD and the Southern Company) were not wholly dependent upon derivatives of the Quipu implementation. This demonstrates the market dominance that these early Quipu derived products have gained. During the last few years a significant number of major suppliers have announced or have released X.500 products, so we can expect this situation to change in the future. An up to date list of available X.500 products is periodically published by the IETF [1], and EEMA expects to publish one in early 1996.

Organisation	Sector	Country
Control Data Systems	Software Supplier	US
Digital Equipment Corporation	Computer Manufacturer	Switzerland
Edinburgh University	Education	UK
EUNet	Network Services Supplier	Germany
INESC	Computing Research	Portugal
Ministry of Agriculture and Fisheries	Government	UK
North American Space Agency	Space R&D	US
Southern Company	Electric Power Generator	US
SURFnet	Network R&D	Netherlands
University of Adelaide	Education	Australia
University of Texas	Education	US
US DoD	Government	US
National Health Service*	Health	UK
UK MoD*	Government	UK

Table 1 Organisations participating in the X.500 survey

3 The Survey

The survey was carried out in two stages. The first survey took place during the summer of 1994, and a follow up survey was conducted a year later. Over a hundred organisations were initially contacted, either through personnel contacts, product suppliers or via Internet electronic mailing lists. The majority of these organisations were commercial or university organisations, but the US DoD and the UK MoD were also approached. Eventually 28 organisations agreed to respond to the survey, but only 15 completed responses were finally received. The case studies were performed entirely over the Internet, and the methodology that was used for collecting the case study material is presented in [17].

Organisations were sent the questionnaire shown in Appendix 1. Thirteen detailed responses were received to the first study, and a further two to the follow up in September 1995. The organisations who responded are shown in Table 1 below (an * indicates the 1995 respondents). Approximately half of the original respondents updated their responses during the second stage. Summaries of the 15 cases are described in section 0.

4 Important Lessons Learnt from the Case Studies

This section contains the important findings from the case studies. Whilst all of the factors described below affected the implementations in one way or another, only a few of them were critical to the success of the project. Critical is used to describe a factor whose absence or mismanagement would seriously jeopardise the successful outcome of the implementation. The factors which were found to be critical were data management, top management support, and integration with other applications.

4.1 Data Management

Data management is one of the most important issues in building a successful X.500 service. Users will be very unhappy if they find that the directory information they seek is either out of date¹ or not present when it should be. Data management comprises of the initial bulk loading of the directory followed by the ongoing day to day maintenance of the data. Several organisations **significantly underestimated** the importance of this issue and the amount of effort involved in collecting and maintaining the directory information. For example, the Southern Company took approximately 3 weeks to load their data into their DSAs, even with the help of bulk loading software tools. Also, in another case, the collection of directory information had to be repeated because out of date information sources had originally been used.

4.1.1 Bulk Loading from External Databases

All the organisations studied in this survey, except MAFF, took the approach of bulk loading the directory from external corporate databases, and all had to provide, at least to some extent, their own custom built tools for the process. The only exception was the Dutch SME pilot. (Note: the Digital bulk loading tool is supplied to its customers, and this was used by the Southern Company to load all of its DSAs). Many organisations had to take the data from more than one source. For example, Digital took information from the personnel database, the MTS routing database, a site facilities database and a central node registration database (containing details of more than 100,000 network nodes). NASA imported data from various relational databases and the phone books. Control Data took data from the Human Resources database and the E-mail database. The NHS took data from the Royal Mail postal regions file, the DoH X.400 address book and Organisation Codes text file. Problems can arise when the different databases use different unique keys. For example, at Delft they found that in two different databases (Human Resource and telephone number) which held people's names, only 60% of the names were identical, due to misspelling, reversed or missing initials etc. Therefore over 2000 entries had to manually compared.

¹ An interesting corollary of this was that one organisation which updated its X.500 directory daily from the Human Resources database, found that during a downsizing and restructuring exercise, entries flagged 'redundant' in the HR database were deleted from the directory before the member of staff had officially been informed of his imminent departure.

Furthermore, one needs to be aware that the corporate database may not always be complete or accurate. For example, the University of Nijmegen found that casual and externally funded staff were not held in the central staff database, and therefore these had to be individually input by the local administrator. The NHS found that their Organisation Codes file was full of errors, such as: incomplete entries, non-standard abbreviations, and duplicate but slightly differing entries. Manual corrections to the 8000 entries took 2 man weeks of effort.

4.1.2 Ongoing data maintenance

There are no hard and fast rules for how this is administratively achieved. The style of data management that is adopted appears to be specific to the structure and culture of the individual organisation. Digital used centralised management for the basic DIT, but allowed users to update selected attributes themselves. Nijmegen, a highly decentralised organisation, devolved data management to the administrators in the individual organisational units, but did not allow users to update the information themselves. NASA devolved data management to each of its 20 sites, and allowed users to update certain attributes themselves. Control Data update the data centrally from the HR database, but allow the Help Desk to validate the data and the users to update limited fields. One complaint raised by a user of the directory at a site where users are allowed to update their own entries in the DIT, was that some users did not bother to do so, and this caused frustration to the other users seeking the correct information. Many universities, the MoD and the NHS centrally manage their directories, and users are not allowed to update their entries.

The conclusion must be that there is no single preferred method for the style of data management. It would seem to depend upon the structure and culture of the organisation in question.

Frequency of updates also varied between respondents, but was typically either daily or weekly, depending upon the source of the data. Occasionally data was updated monthly, and once (for the photograph attribute of Delft students) the answer was annually.

One factor that is common to all of the studies however, is that data management can be time consuming and expensive. NASA estimate that it requires 0.5 FTE (full time equivalent) per site for data management. Texas quote a figure of 0.125 FTE. Other figures are given in 3.3. However, one should always try to de-couple the costs of data management that are independent of X.500, such as managing the Human Resource database, from those which are directly attributable to the support of X.500. Digital noted that it already had extensive processes for managing the data which were justified independently of X.500, and were properly supported within the organisation (via management policies when necessary). This made the loading of the X.500 directory much simpler.

All organisations agreed that keeping the directory information up to date is critical to the success of the pilot or operational service.

4.2 Data Richness

All X.500 projects except MAFF and the NHS stored postal addresses, telephone numbers, fax numbers, and E-mail addresses for people. MAFF initially only stored E-mail addresses, but were due to add the others during 1995. Many organisations added their own specific attributes, for example the Digital directory stores locally defined attributes such as: VMS mail addresses, 3 letter location codes, and employee status. The NASA directory has a 'NASA Recipient' attribute. The EDF directory has photographs and voice attributes. The REDACS directory had a number of attributes which were specific to REDACS. Adding organisation specific attributes would seem to cause no problems to the respondents. In fact, this could be seen to be one of the strengths of having an X.500 directory service.

A number of the directory projects were integrated with their E-mail systems and these usually stored E-mail attributes such as: mailing lists, O/R addresses and PSAPs etc., and a number of projects are experimenting with storing MHS routing tables.

One pilot report suggested that administrators should try adding some useful information to the directory, that was not readily available elsewhere. This would help users 'buy into' the service. As an example, the report suggested that a research organisation might add the attribute 'field of research' to its people entries. It should be noted that this suggestion came from a site that did not have integrated E-mail user interfaces, and as suggested in section 3.3 this would seem to be essential for high user acceptance.

4.3 Integration with other Applications

Integration with E-mail, or some other communications service, would seem to be of paramount importance in order to get high user acceptance of the X.500 directory. Where integration was achieved, e.g. REDACS, MAFF, Digital and Control Data, the sites reported almost universal use of the X.500 directory, even though users were often not aware that they were accessing X.500. Conversely, patchy use was reported where integration with E-mail or some other communications service, was not achieved. Nijmegen had hoped to achieve E-mail integration, but found that because there were no products available off the shelf for this, they had to drop this requirement from their pilot. Texas, who reported good usage of X.500 because of integration with existing user interfaces, still only had a fraction of the usage of those organisations where E-mail was integrated (1 access per 5 people per day for Texas, as opposed to 15 accesses per person per day for Digital).

Several respondents said that the inability to link the mail and directory systems together was a severe limitation. The DoD stated that their first principle is that users prefer to access the directory from within their familiar mail user interface, and this therefore is a mandatory feature of DMS. Adelaide quoted integration with cc:Mail and SMTP as important features to have.

Electronic mail is not the only communication service with which the directory has been successfully integrated. In REDACS the directory is used in support of the management of transport layer connections, and Texas are using X.500 integrated into WWW, Gopher and Finger.

The conclusion must be that an integrated mail (or other communication service) and directory interface is critical for wide user acceptance and use of X.500. There are many potential solutions to this, which are suggested in the various responses, but not all of these may be available in any given situation. The potential solutions are:

- i) buy a manufacturer supplied E-mail/X.500 integrated interface and migrate users to this;
- ii) build your own integrated interface and migrate users to it;
- iii) buy or build synchronisation tools that populate the existing proprietary E-mail address book (post office) with the contents of the X.500 directory;
- iv) interface the X.500 directory to the, possibly proprietary, directory API provided by the E-mail user interface;
- v) provide a special purpose service, e.g. the REDACS name service, which caches directory information to interface to users.

The current cases would tend to suggest that options ii) and iii) were the most likely solutions adopted by the early pilot reported here, but the author anticipates that options 1 and 4 will become more prevalent with time. Option v) may also become more relevant in certain environments, in particular where performance issues become more critical.

4.4 Costs and Timescales

Few organisations were willing to give complete costs. Digital did provide commercial in confidence information to author which was forwarded to the project sponsors.

NASA quoted 1.25 million dollars per annum total maintenance and support costs for their 20 sites. The implementation took one year and cost 1.2 million dollars.

EDF quoted 2 million French Francs for their research centre directory service.

Control Data quote 1/3 million dollars total support costs per annum for their global system. Implementation figures are not given, except to say that the project took longer than the original plan of one year.

Nijmegen forecast 220 man days for setting up their basic service, writing the software tools, solving the organisational and administrative issues and managing the project, which lasted for just over one year. They also allowed 100 man days for the 9 organisational units involved in the pilot, for managing their portions of the DIT and supporting their users over this period. In fact the project took 230 man days for the basic service, but less than 100 man days for the organisational units.

Texas would seem to be one of the star performers, taking only 3 man months to install their system.

4.5 Project Management

4.5.1 Project Sponsor/Top Management Support

Each X.500 project that had a project sponsor and top management support was deemed to be successful. Digital's project had the Corporate Information Officer as its sponsor, Control Data had the general manager of MIS. The DoD project manager remarked that the support of the highest level of senior management was an invaluable asset to their project.

The only respondent whose project has been an almost total failure to date, was one who did not have top management support. This was Edinburgh University, where the project was originally started by the Computer Centre technical staff. When they came to ask the University management for data for the directory, the University management stated that the staff list was private to the University, and therefore could not be published in the X.500 directory. The pilot service was therefore only capable of listing 1% of staff names, these being the members of the Computer Centre.

The conclusion must be that top management support is a critical success for an X.500 project.

Highly decentralised organisations, that operate as autonomous units (most universities fall into this category) also need to get the commitment of (possibly many) different groups of stakeholders in order for an X.500 project to be successful. Considerable effort may need to be expended in this area, and this should not be overlooked.

4.5.2 User Involvement

It is interesting to note that 'high user usage of the final system', or a similar reason, was not given as the goal of any of the projects studied in this report. Since many of the projects were no more than proof of concept or pilot services, one should not be surprised that very few of them had any user involvement from the outset, or that any of them had defined any metrics for measuring user acceptance and usage. These quality criteria can be expected as X.500 becomes more established. In most cases, the eventual acceptance of the final system did not seem to be effected either way by lack of user involvement in the project. For example, in the case of NASA, final user acceptance was reportedly good, but in the case of Adelaide and Nijmegen they stated that usage would have been much higher if an integrated E-mail interface had been provided.

Conversely, if the users were involved from the outset, then in the small number of studies where this was the case, the users would have a high acceptance of the final system. This was evident in the case of Digital, where user acceptance of and feedback about the final system was good. In this case the users were involved in defining features of the service during the requirements analysis phase.

The only project to have carried out a comprehensive survey of user experiences was Nijmegen. In 1994, they circulated the 2000 users with entries in the directory and obtained a 29% response rate. The main group of these who used the directory turned out to be computer literate staff who already used E-mail. The users were reasonably satisfied with the command line interfaces, Gopher and DE, but were much more satisfied with the Max500 graphical user interface. They asked that Web and MS-Windows interfaces be added (the Web one has since been added), as well as interfaces integrated into their existing E-mail packages. Many users said that they were unaware of the existing service, despite frequent notices in User Bulletins etc. publishing the fact. One can conclude from this that a stand-alone directory interface is much harder to get established in the user community than one that is seamlessly integrated into existing applications.

4.6 Name Registration

Not all organisations have endeavoured to register their directory names. They have chosen the name that seems most appropriate to their organisation, and may register it if/when this seems appropriate. For multi-national organisations such as Digital and Control Data, there currently is no mechanism for registering names below the root of the directory tree, and so both organisations have pressed on regardless. ITU-T are currently working on a recommendation for the registration of international organisations [7], but this is not yet complete.

The DoD on the other hand, has a very strong name registration scheme, being named below the arc Country=US, Organisation=U.S. Government, Organisational Unit=DoD. Internal documentation has been produced detailing the policy and procedures that should be adopted throughout the organisation. Likewise Texas followed the NADF guidelines, and registered their name with ANSI. Edinburgh registered its name with DISC, which operates the UK name registration scheme on behalf of BSI, as this was recommended by the original project sponsor (the JNT).

The lack of using a registered name has caused problems to one of the pilots, and is a potential problem to another. The NHS had to change the name of its organisation's entry from 'NHS' to 'National Health Service' when they connected to the NameFLOW-Paradise public service. This was a major inconvenience to them as it meant that every entry (>10,000) in their directory had to be updated to reflect this. MAFF require everyone who is connected to their X.400 service to be registered in their private X.500 directory, and this applies to external people as well as employees. An external person who already has an entry in the public NameFLOW-Paradise service is given a second private entry in the MAFF directory, usually with a different name. This will cause MAFF a problem if and when they decide to connect to the public directory service.

Choosing a sensible naming structure for the whole organisation may prove difficult. This was the case with the NHS, given the preponderance of organisational units with the same name e.g. St Mary's Hospital. It was eventually decided to model the directory naming tree on UK postal regions as defined by the Royal Mail, as it was realised that this was a much more stable

structure than the internal organisational structure of the NHS.

4.7 Technical Problems

This section addresses the technical problems associated with installing and configuring the directory systems (DSAs), and then in inter-connecting different systems together. Whilst these problems may be time consuming and frustrating to solve, they are usually not insurmountable, nor critical to the success of the implementation.

4.7.1 Installation Problems

Several sites reported that installing and configuring the X.500 software took longer than planned. This was particularly apparent with the Quipu software, which only had a limited amount of very technical documentation written by experts, which is hard for non-experts to understand. Nijmegen had a 50% overrun on technical tasks, taking 650 hours instead of the planned 400 to complete the project. One respondent from a European University, not otherwise included in this survey, said that he had tried to install Quipu but couldn't and so had finally given up. The NHS reported 'a great many problems in bootstrapping the DSA', though they did report that newer releases from Nexor have improved. NASA on the other hand took 20 days to install 20 Quipu systems, but it has to be remembered that this was undertaken by highly experienced people who had been 'playing' with Quipu for a number of years prior to the project. Similarly Texas, who had originally planned their project to last for 1 month in total, installed Quipu in 2 days, but eventually finished their project in 3 months due to data loading problems.

At the opposite end of the scale Digital reported that their DSA installation time was just 30 minutes. This was qualified by the assumption that the person installing the DSA already has some knowledge of Digital's OSI implementation, DECnet/OSI, and that this had already been installed. The Quipu respondents were quoting the total time to install ISODE and Quipu. A useful distinction to make would be between the complexity of setting up an OSI transport service and setting up an actual DSA. Setting up the transport service is usually the toughest part, but unfortunately this survey did not ask the respondents to differentiate between the two tasks.

In the case of two projects, REDACS and Southern Company, the installations had been set up by outside contractors who handled the problems of getting the directory up and running. They therefore reported no technical problems with the installations.

4.7.2 Interworking Problems

Once the DSA is installed it may then be necessary for it to communicate with other DSAs. One might expect problems to arise when the DSAs are from different manufacturers, and indeed this was the case as experienced by the Southern Company. The HP DSA would not initially accept a connection from the Digital DSA. It took time to determine the reason and rectify it, and this caused delays to the testing schedule. Worse still, the Telstra DSA and Unisys DSA were unable to communicate for the duration of the project. However, the

manufacturers can be expected to fix this problem in a subsequent release of their products.

One would not expect interworking problems to exist when connecting together two DSAs from the same supplier. But this proved not to be the case. The Southern Company had interworking problems between two Telsta DSAs, and the NHS had problems connecting their Nexor Quipu DSA to the NameFLOW-Paradise service which also uses Quipu DSAs. Again, these sorts of problems can be expected to diminish as later releases of the products are issued.

4.8 Legal Issues

Organisations do have legal requirements placed on them, via their national Data Protection Acts, for the storage of personal data. Some organisations (e.g. Nijmegen) took the view that the information held in the directory was personal data, and so wrote to each employee allowing them to opt out from having their name and related information stored in the directory. (In fact very few employees chose to go ex-directory.) Other organisations took the view that the information stored in the directory was purely corporate information, and employees were not asked for their permission. Indeed one organisation said that it was part of the employee's terms and conditions of service that their information was held electronically by the company, implying that they would not have a job if they objected to their data being included in the corporate directory. Texas had a similar clause for its students and staff.

Organisations did notify the Data Protection Registrar when it was deemed necessary to do so.

Recent work performed subsequent to these case studies has revealed that some countries are now taking a different viewpoint of electronic directory data, depending upon whether the corporate directory is connected to the Internet (i.e. NameFLOW-Paradise) or not. If connected to the Internet, then the directory service provider may need to get the written permission of every person before his/her details are stored in the directory. One organisation in Germany, GMD, has had to remove its directory from the NameFLOW-Paradise service because of data privacy issues and objections by the employees federation.

4.9 Response Times

All organisations found that response times for data retrieval from their local DSA was acceptable. This was typically of the order of 1 or 2 seconds, with the worst case (INESC) being 10 seconds. In the case of Digital, responses from the local DSA could be almost instantaneous, and only up to 3 seconds for data from a remote DSA within the organisation. NASA reported 2 seconds for local queries and up to 35 seconds for queries to remote DSAs within the organisation.

Many organisations found that response times were very variable and often unacceptably long for data retrieval from remote organisations that were accessed via the public (NameFLOW-Paradise) service. Typical values measured at Salford University ranged from 3 to 30 seconds for other organisations in the UK, and sometimes many minutes for data from the US.

Clearly organisations have no control over response times from the public directory service, but it would seem to be possible to achieve eminently acceptable performance levels for intra-organisational data retrieval. The worst case figures, for running say 20 Quipu DSAs throughout the organisation might be around 30 seconds. External accesses would be worse than this, but the authors are aware that Dante, the organisation now responsible for managing the public NameFLOW-Paradise service in Europe, are currently evaluating mechanisms for improving the performance of the public directory service.

REDACS have devised another solution to performance related problems with the directory. The REDACS directory information is cached in a special purpose name server indexed for fast access of user information. Retrieval of the directory information is by simple look-up of the index information which is encoded and passed to the user using special purpose protocols. The name server's copy of the users directory information is generated as and when required by the local management facilities on the servers. This type of solution could be applied by other organisations where performance is paramount.

4.10 User Interfaces

Some organisations built their own user interfaces, whilst others made do with what was publicly available. At the end of the day this would seem to be a matter of cost and of the resources that the organisation has to spend on the X.500 project. Those organisations which had the resources and the will to succeed, e.g. REDACS and EDF, built their own interfaces, particularly integrated ones, whilst those organisations which did not have the resources e.g. Nijmegen, had to make do with lower quality publicly available interfaces, and perhaps with less users migrating towards X.500.

The big change that has been seen in the twelve months between the two surveys, is the adoption of WWW browsers as a predominant means of accessing the public X.500 directory. The University of Texas have quoted a change from 80% Gopher access in 1994 to 22% Gopher and 66% Web access in 1995.

4.11 External Access

All organisations responding to the survey, except REDACS, wanted to allow their users to have access to the global public directory, but not all of them wanted the public to be able to access their X.500 directory! Universities (and NASA) typically were the only organisations giving public access to their information. The commercial companies, Digital and Control Data, as well as the DoD, EDF and the NHS, were only prepared to let the public see a tiny fraction of their directory entries. It will almost inevitably be the case that the only information that will be available about many organisations in the public directory will be little more than their name and phone number (as in today's paper directories), and the remaining information will be hidden from public view.

4.12 Security Considerations

Organisations dealt with security issues in different ways. Perhaps the most simplistic approach, adopted typically by universities, was to say that all information in the Directory was for public read-only consumption, and that only the administrator could update the information. In this way it was not necessary to authenticate any of the users, and passwords did not have to be stored in the directory. Access controls are also much simpler to administer. This scheme was adopted by a number of universities e.g. Nijmegen.

Another simplistic approach is to restrict directory access to employees only, and to not connect to the global public directory service. MAFF initially adopted this scheme, and so have REDACS. The DoD has considered a variation of this, whereby the directory is partitioned. One partition, holding all the directory information, is for employee access only and is not connected to the external environment. Another partition, holding a subset of the directory information, is for external users and is connected to the external environment. DSAs may not communicate between the partitions, so that the DoD has complete control over what information is made externally available.

More complicated access control schemes become necessary once an organisation wishes to connect to the public directory service, but wishes to limit the amount of internal information that is made available to the public, or once an organisation wishes to allow its users to update a subset of the directory information. Access controls need to be set at the attribute level (or value level), in order to tightly control the information that users can access.

Once users are allowed to update their entries they need to be authenticated, and password management, or an alternative, becomes necessary. This was implemented by a number of organisations e.g. Digital and NASA. Some organisations used Kerberos authentication with LDAP user interfaces, as an alternative to simple passwords. NASA was the only respondent to have limited operational experience of strong authentication (digital signatures), although the DoD is also known to be experimenting in this area.

In conclusion, security considerations add a level of complexity to the management of directory services, and for this reason many organisations are treading carefully here. Another reason for being cautious is that products are not yet 'security mature', since access controls only appeared in the 1993 version of the standard.

4.13 Protocols

Several organisations used a variety of protocols for interconnecting between DUAs and DSAs, e.g. pure DAP and LDAP, and between DSAs and DSAs e.g. TP4/CLNP/802.3, TP0/CONS/X.25(84) and TP0/RFC1006/TCP/IP.

All organisations used LDAP [8] for at least some of their user interface accesses to their DSAs. However, the Southern Company noted one problem with this. LDAP does not support the *dontUseCopy* service control, and they found that 'out of date' cached (copied) information was being returned after an entry had been updated. Consequently there was no

way of asking for the original source of the information. This would pose a problem when it is essential to have the most current information from the directory.

All organisations except MAFF used RFC1006 [9] for interconnecting at least some of their DSAs (this is not surprising, since this is the main protocol used by the NameFLOW-Paradise and US White Pages pilots).

The big change that was noticed in the twelve months between the surveys, was the appearance of products conforming to the 1993 edition of the X.500 standard, and in particular the use of the shadowing (DISP) protocol for replication, instead of proprietary ones.

The good news here seems to be that the ISO 7 layer model works in practice as well as in theory, and that lower layers can be switched without affecting the functionality of the upper application layer.

5 The Case Studies

5.1 Control Data Systems

Control Data Systems have an operational X.500 service which uses their own in-house technology. The original DSA was based on Quipu, but the new one is a 1993 compliant product, that inter-operates with the old system. The 1993 product was introduced into their corporate directory service in September 1995. The corporate directory is integrated into their X.400 E-mail system. The directory system comprises of approximately 15 DSAs and holds details about all 3,500 Control Data employees, as well as distribution lists, and an X.400 configuration and routing tree. The system is used by virtually all the employees for telephone number look-ups, as a replacement for the paper telephone directory, although exact usage statistics are not kept. Response times are said to be good, in the order of 1-3 seconds per lookup.

Some of the E-mail interfaces have had X.500 access transparently built into them, so that users are unaware that X.500 is being accessed behind the scenes. For other interfaces this was not possible, and so these users still have to access X.500 from a stand-alone interface. Never-the-less, Control Data claim that the current system is still saving them over 10 dollars per month per e-mail user in system support costs. The latest interface to be introduced is WebLink500, which allows any World Wide Web browser to access the X.500 directory.

5.2 Digital Equipment Corporation

Digital have an operational in house directory service based on X.500, using their own X.500 technology. The goal is to replace the many diverse and proprietary directory systems that they currently have, with one single homogeneous X.500 system. This is an ongoing process within Digital, and will take many years to complete. The X.500 system currently holds data for each employee (60,000 in September 1995), and for many applications, computer systems

and network entities (totalling nearly one million). The latter will expand, as the eventual aim is to hold 10 million entries in the Digital DIT. The system currently comprises of 30 DSAs around the globe, and will eventually expand to over 100. The system is judged by Digital to be a great success because each employee on average uses the directory 15 times a day. Several X.500 user interfaces are employed. Some interfaces are standalone, whilst others are integrated into application services such as: ALL-IN-1, World-Wide Web (WWW) and Videotex. User migration to X.500 was found to be very easy to achieve when the X.500 interface was a direct replacement for an existing proprietary directory facility. In some cases the users were hardly aware that a proprietary directory technology had been replaced by an X.500 based one. User queries are answered on average within 3 seconds, with a large majority being within 1 second.

It is anticipated that the greatest use of X.500 inside Digital will eventually be made by applications, for example, for MHS routing. Current usage figures of proprietary directories and name servers in Digital show that user look-ups account for just 1% of directory accesses. With current X.500 accesses running at over 1 million operations per day, Digital clearly expect their X.500 service to be capable of much greater things in the future, once the current roll out is completed. For example, the target date for X.400/X.500 integration is June 1996, and usage is expected to dramatically grow after this date.

5.3 Edinburgh University, UK

Edinburgh University is the only case study in this series, which is currently judged by its respondent to be a failure. Whilst the project had the backing of the management of the computer centre, it did not have the full backing of the top management of the University. Software (Quipu) and hardware (Sun) were donated to Edinburgh by the JNT, a central funding body for networking in UK universities, and these were installed in due course. The problems arose once the computer centre wanted access to the University database in order to bulk load the directory. The University management stated that the staff list was private to the University, and therefore could not be published in the X.500 directory. Consequently the project ground to a halt for a number of years. In 1994 the University reversed its decision, and it was hoped to load the directory later that year. But lack of both resources and impetus meant that that was not achieved. Edinburgh will probably now wait for a shrink wrapped directory solution from a company such as Novell or Microsoft before implementing a corporate electronic directory service.

5.4 Electricity de France

EDF has three directory projects, in various stages of development. The most advanced project is currently operating across the 4 research centres in Paris, which employ 2500 people. The two year project, which started in 1994, will give all the research staff access to an X.500 multi-media directory service. The directory contains not only the standard attributes such as telephone numbers and Email addresses, but also photographs of employees, maps of locations, and voice recordings. It is planned to add video in the future. Information about organisational units accounts for nearly a third of the entries in the database. Access is being

provided via Web browsers running on a variety of workstations - Apple Macintoshes, Unix workstations and PCs - as well as via an interface integrated into E-mail. A significant amount of the development effort has been expended on the user interfaces and the management interface, both of which have large amounts of bespoke software in them. The system is partially connected to the public NameFLOW-Paradise [10] service, so that the public has access to a limited number of EDF entries, but the employees cannot currently access Paradise. Strong authentication has been implemented.

The second project is longer term. EDF employs over 160,000 staff, not only in France, but scattered throughout the old French colonies, and so a truly global directory service is required. A number of different proprietary directory technologies are currently in use throughout the organisation, but they all contain differing amounts of information. The aim is to synchronise all of these various directories together, possibly via an X.500 backbone. The project employs 10 staff at the moment, who are working on the design of the global system. Prototyping with X.500 is currently under way, to see if it is capable of the task. The project started a year ago and is planned to last 3 years.

The third project is even longer term, and is currently only at the architectural design phase (which is itself planned to last three years). EDF are part of a consortium, comprising INRIA, Banque National de Paris and France Telecom, whose aim is to specify an advanced object oriented information system capable of supporting work groups and transaction processing. An X.500 directory is at the heart of this, for storing information about users, applications, and documents etc.

5.5 EUnet, Germany

EUnet is one of the leading Internet service providers in Germany. It has offices in most European countries, but only two of them, Germany and Ireland, have experience of implementing X.500. The German unit, which responded to the survey, started to experiment with Quipu in 1994, and therefore has limited experience of using X.500 in an operational environment. In 1994 one person spent about 3 months installing Quipu and interfaces to other data services, e.g. to Gopher and WWW. They also loaded a limited amount of data, including photographs, into the system, but since there were only 34 employees in Germany, this was not a huge task. (Note that in the following year the company grew to 81 employees, and this data has been subsequently added to the directory.) EUnet have also experimented in loading MHS routing information for the EUnet/DFN (German Research Centre) into X.500. This routing information holds mappings and routing information for the SMTP/X.400 Gateway and for X.400 Relaying. (EUnet currently holds this information for the DFN in proprietary look-up tables). It is too early to say if this experiment is a success.

5.6 Instituto Engenharia e Sistemas e Computadores (INESC), Portugal

INESC is a Portuguese R&D organisation employing 1200 employees across 5 major cities. In 1994 it completed a 12 month project to install an ISODE Consortium (Quipu based) DSA. This centralised system holds information about all of the employees as well as entries for its

E-mail application (5000 entries in total). Users were not consulted about the introduction of the service, as the intention was to initially provide a stand-alone telephone and E-mail directory look-up service, and then find out later from users what features they would like to have added to the system. Consequently use of the system was only small in the beginning, but it grew fivefold during the first few months of operation, and is currently estimated to be about 5000 operations per day (although statistics are not kept).

The other main use of the system is as a vehicle for research. One interesting project is using the directory to store photographs for security purposes. Photographs of employees are stored in their directory entries and this is then linked into the security detection system of the buildings. Security guards are able to retrieve the photographs of people for authentication purposes. Another research project is trying to generate voice responses to X.500 directory requests (similar to the current telephone directory enquiries service in the UK).

5.7 MAFF

The Ministry of Agriculture Fisheries and Food is a widely dispersed organisation occupying over 200 sites throughout the UK. Each site is connected via X.25, and they have had an integrated operational X.400 and X.500 service for nearly four years. The current number of DSAs is 22, and this is expected to rise to 30 by the end of 1994. The directory system is a derivative of Quipu, and is supplied by an Irish software house. MAFF have developed their own integrated X.400/X.500 administrator interface (called MICE), and adapted a commercial Windows based DUA/UA interface for their own use. The directory system currently holds O/R addresses, Unix usernames and X.400 routing tables, and will be expanded to hold other useful user information such as telephone numbers. This project is a major success because integration of X.400 and X.500 was always a key driving force. Users are not allowed to use X.400 before they are registered in X.500. However, this does potentially lead to a technical problem (see 0).

5.8 National Health Service

Phase 1 of the NHS pilot took place during the first 9 months of 1994. The main objective was to gain practical experience of installing and managing an X.500 directory in a 'pseudo-real' environment. To this end, details of about 8000 NHS organisations (hospitals and GPs) and 2500 X.400 users were loaded into a DSA provided by Nexor. A variety of interfaces were installed and tested, including windows based ones and dial-up modem access via the DE package from UCL. User comments on the whole were positive, but this might be as expected given that the NHS does not currently have access to any other similar proprietary or non-proprietary directory service. The main problem encountered during the pilot was data management, since the NHS did not have access to good quality data. The raw organisational data contained lots of errors and ambiguous duplications, and it was a major task to load the directory database.

Plans for Phase 2, which will include the piloting of 1993 directory features, are currently underway, but the pilot is not expected to start until early 1996.

5.9 NASA

A NASA employee originally started experimenting with X.500 (Quipu) in his spare time, and this eventually developed into a multi-million dollar project whose outcome, in June of 1994, was an organisational wide X.500 system holding all 100,000 NASA employees. The system spans 20 DSAs located at various sites all over the US. The DSAs are supplied by the ISODE Consortium and Control Data, both of these being Quipu derivatives. In 1994 the system supported 40,000 operations per day, which represented a growth of 400% over the previous year.

Prior to the start of the project, in June 1993, NASA only had a few experimental Quipu DSAs deployed, whose data content was variable. The current project has enabled the whole organisation to be represented in the X.500 DIT, and for all employees to have access to an organisation-wide electronic directory service, via both stand-alone and integrated user interfaces. A judge of the success of the project may be gained from a comment of the project manager, that 'users are delighted to have a working agency-wide phone book, and they are upset whenever there are outages'.

5.10 The Southern Company, US

The Southern Company pilot is very different from the other case studies in this series, in that it is primarily concerned with X.500 interworking between different vendor systems. The Corporation for Open Systems International (COS) are the prime motivators of the project, and the Southern Company, one of the US's largest electric utility groups and a COS member, volunteered to be the subject organisation. The information contained in this section was obtained from COS copyright documents [4, 5, 6], and the author thanks COS for their kind permission to draw from them.

The project is divided into three phases. Phase I, the user requirements and high level design, was completed in 1993. Phase II, the proof of concept, was divided into three stages and completed in March 1995. Phase III, which is the deployment of a fully operational X.500 service, may be elected by the Southern Company at a future date, partially based upon the results of Phase II.

Stage 1 of Phase II took only six months to complete, and finished in June 1994. Stage 1 made the E-mail addresses, for a subset of Southern Company employees, available via X.500. In addition, E-mail addressing information was successfully synchronised between X.500, ALL-IN-1 and Microsoft Mail. The multi-vendor nature of the project was ably demonstrated through the Southern Company DIT being totally held in a Hewlett Packard DSA, but the synchronisation with ALL-IN-1 and Microsoft Mail was performed via a Digital DSA. External connections to a Unisys DSA located at COS were also provided. A full report of this stage can be found in [4].

Stage 2, which successfully completed in September 1994, significantly expanded the work of

Stage 1. The Southern Company DIT was distributed between Digital, HP, Unisys and Telstra DSAs, and connected externally to Nexor DSAs at the Electric Power Research Institute, Unisys and Control Data DSAs at COS, and a Telstra DSA representing Country=Australia. Nine DSAs in all were involved, and they were a mixture of 1988 and 1993 conformant products. The Southern Company DIT was populated with approximately 50,000 entries (spread over its 4 DSAs) and these were downloaded from an extract of the company's human resource database (SHIPS) and proprietary E-mail directories via Digital's Directory Synchronizer product. Structured interworking tests were then performed between these DSAs. Administrative DUAs were used to update the DIT information in the different systems, and user DUAs were used to retrieve information from various sites. Dozens of tests were performed, and the majority, though not all, completed successfully. Because of the number of systems connected together, it had been hoped to be able to initiate concurrent operations to see how the DSAs performed both under load and when the requests conflicted (e.g. concurrent read and update operations). Unfortunately there was insufficient time to carry out the concurrent testing. Never-the-less the tests proved that X.500 products from different vendors, utilising different platforms and software implementations, and supporting different versions of the Standard, can successfully interwork to provide a useful directory service.

Stage 3, which successfully completed in March 1995, extended the functionality of Stage 2 by implementing additional 1988 features such as *organisationalRole* and *groupOfNames* object classes, and 1993 features such as shadowing and schema management. In addition seven different desktop user interfaces (DUA)s were compared and contrasted for usability and flexibility. The 1988 feature testing was very successful, but the 1993 feature testing proved to be too limited, since different manufacturers had implemented different subsets of the 1993 enhancements. Hence the enhancements were usually only able to interwork between two copies of the same implementation. This situation is expected to change radically over the next 12 months as more manufacturers add more 1993 features to their products. Desktop DUA testing covered user authentication, and the searching, reading, and modification of DIT entries. Different DUAs supported different sets of features, and whilst a limited number of bugs were found in a few of the implementations, all DUAs had some notable features. The COS report [6] provides a full description of the tests and results.

5.11 SURFnet, the Netherlands

SURFnet is the organisation which manages the Dutch R&D network. SURFnet were originally involved in three X.500 pilot services. One was at the University of Nijmegen and its associated teaching hospital St. Radboud, the second was at Delft University of Technology, and the third, in conjunction with the Dutch Department of Home Affairs was to set up a central X.500 service for small and medium sized enterprises (SMEs). All of these pilots were built using the XT-Quipu product from Nexor. When these pilots turned out to be successful, 8 more universities joined in. The pilot finally became an operational service in 1995.

5.11.1 University of Nijmegen

The main aims of the Nijmegen pilot were to build an organisational structure and operational

procedures for managing the data that is fed into the X.500 directory, and to investigate if, and to what extent, the X.500 directory could be populated from existing corporate databases. This would involve the identification of organisational roles for the administrative tasks, and the development of administrative procedures and software tools for performing the data management tasks. The resulting mechanisms should be suitable for managing the DIT entries of all the staff and students at the institution. If this was successful, then an operational service could be provided, in the first instance, to some of the staff.

The University and Hospital are highly decentralised organisations, and so a mutually agreed organisational structure and set of operational procedures had to be developed for management of the data. Since data management would be devolved to the units within the organisation, obtaining the commitment of staff in the various units was clearly an important consideration.

Automated software procedures would need to be built for loading the skeleton directory from the two existing corporate databases (one for students and one for staff). Local administrators would then be responsible for validating and fleshing out the final DIT.

When the 15 month pilot was completed in early 1994, 2000 'person' entries had been stored in the Quipu based DSA, and this had been successfully interconnected to the NameFLOW-Paradise public service.

A second project was started in mid-1994. Its multiple aims were to: perform user evaluation of the existing service by sending out a questionnaire to the 2000 registered staff, set up a "Yellow Pages" service, extend the directory to all the staff of the University and to a first group of students, and refine the existing administrative procedures to ensure that the directory will be kept up to date. The user survey was duly completed, and the results are presented in 0. By the end of 1994, 4600 entries were included in the DIT, and this is expected to grow to 6000 before the end of 1995.

5.11.2 Delft University of Technology

The TU Delft pilot had very clear aims, which were to implement a directory with at least 5000 entries, and to gain experience of the technical, organisational and administrative issues that are involved in creating and running such a system. One of their main conclusions was that solving the organisational and data management problems is far more difficult than solving the technical problems. (This conclusion is in line with other research into implementing IT in organisations, for example, in MRP and EDI implementations.)

At the end of the 15 month project (which started in Nov 1992), Delft had built a Quipu DSA holding all the staff of the University and all the students in the faculty of Industrial Design (6000 entries in total), and had fulfilled their objectives. Since user acceptance and usage were not within the scope of their initial project, no statistics have been gathered in this area. This is now the topic of a follow up project.

5.11.3 Directory for SMOs

Small and medium sized enterprises (SMEs) generally do not have the resources or expertise to implement leading edge software in house. Thus the provision of a centrally operated DSA, along with local tools to allow each SME to remotely manage its own portion of the DIT held in the central DSA, would seem to be a valuable service to provide to them.

These were the goals of this Dutch X.500 pilot project, started in late 1992. During its first five months of operation, in the second half of 1993, the number of entries added rose from 100 to over 2000, and the number of directory queries doubled to 2,500 per month. The central system is based on Quipu, and both interactive and bulk loading tools were provided to the SMEs. A number of useful conclusions and recommendations came out of this work, which are presented in the second half of this report.

5.12 University of Adelaide

An 8 month project at the University of Adelaide produced an X.500 service based on Quipu that holds all 4000 members of staff. Bulk loading tools were developed, so that information could be input from the Human Resource database, the PABX, cc:Mail and Unix passwd files. Users are given the freedom to update their own entries, but not many of them take the opportunity to do so. Unfortunately statistics are not kept, so that Adelaide do not know the frequency at which users access the system. The administrator suspects that most of the users actually access X.500 through a gateway from some other application more familiar to them. A snapshot statistic taken specially for this report would seem to support this, as it revealed that 100 binds were made to X.500 during one day (9 hours), and 50% of these came from Gopher.

5.13 University of Texas at Austin

The University of Texas have built an X.500 directory containing all the staff and students at the University (70,000 entries), using ISODE Consortium software (a Quipu derivative). Prior to this there was no organisation wide directory service available, and so when the system was installed in time for the fall 1993 semester, there was an immediate uptake of the service, rising from 2000 requests a day in the fall to 4500 per day during spring 1994. By fall 1995 connections had risen to 15,000 per day. The interesting thing to note about user acceptance is that only existing user interfaces, such as Gopher and Finger, were used. In 1995 Web access was added. These were interfaced to X.500 at the back end so that users did not have to learn anything new; X.500 access came as a 'free' value added service. Now the users are asking for more features, such as the ability to update the information themselves, and to be able to retrieve more information by using more generic searches.

Texas did find that their DIT size was pushing at the upper bounds of the Quipu implementation. They had to write custom loading software and purchase more memory in order to get the system to work. They also have to restart the system twice a day due to 'memory leakage' in Quipu.

5.14 US Department of Defence

The US DoD have been working on the Defense Message System (DMS) for a number of years, and its goals are to provide a commercial-grade secure X.400 and X.500 service, as well as interworking between all existing DoD messaging systems. Clearly an organisation wide directory service is at the heart of such functionality. To date, the DoD have established a Proof of Concept (POC) Directory Service, based on Quipu, which has provided them with valuable technical and operational experience. The POC cannot be described as a true pilot service, due to the limited amount of data that it contains (less than 100,000 entries in 8 DSAs), and the number of users who can access it. Nevertheless, in 1994 the DoD issued a multi-million dollar DMS Request for Proposal (RFP) which requested manufacturers to tender for supplying operational DMS systems. The DMS contract was finally awarded to Loral in summer 1995.

The proposed DMS X.500 directory service is one of the most complex services studied in this report. The DoD have many special requirements over and above the usual name to address look-up services provided by the other respondents' systems. Strong authentication is a mandatory requirement, so is mailing list expansion, mail protocol translation functions, and integrated mail/directory interfaces. Much of the groundwork for the service has already been laid during the Proof of Concept phase, with the production of software tools, schema specifications, registration procedures, training plans, deployment plans and operational and administrative procedures. It will be interesting to follow how this service unfolds in the coming years.

5.15 UK Ministry of Defence REDACS project

REDACS is a layer 1-4 communications service which uses the directory in support of controlling the establishment of connections between users and applications. For each user the directory holds a list of applications that he may access. This information is used to control access between users and applications, feeding into a menu for users to select the application they require and providing the network addresses needed to access individual applications. The directory is also used to hold password information to authenticate users.

Connection establishment is supported through a special purpose "name" server which holds a copy of directory information obtained from the X.500 directory service. This name server obtains information from the directory about all users in its area and the application servers they use. This information is restructured and encoded in the name server to optimise the search time and storage requirements. In addition, a special name server access protocol is used which is optimised for the operations required to control the establishment of connections across REDACS. Through this approach the sub-second performance requirements can be met. If users were to access the directory directly for connection establishment control it would not be possible to meet the design aims (about 5 seconds was

the estimated access time for directory access).

In addition to using the X.500 directory in support of connection establishment, operational users can access the directory directly to obtain conventional directory attributes (phone numbers etc.).

Plans are underway to extend REDACS to support X.400 interpersonal messaging with direct use of the X.500 to support X.400 addressing. REDACS are planning to use the schema defined in X.402 to support the X.400 service.

The X.500 directory itself is currently fully replicated across several DSAs (one for each of the 9 areas) with an additional central DSA which holds a master copy of the entire directory information. All the DSAs are provided by Unisys. Updates are carried out on the master copy for all attributes except passwords, for which special procedures are applied. Information on updates carried out on the master copy are passed on to the shadow copies on a daily basis using proprietary means. It is planned to use the X.500 1993 shadowing protocols to replace the existing proprietary approach to replication.

Whilst the use of the directory is unusual in REDACS, the X.500 directory service has been found to be useful for maintaining structured information on network users and services. It has, however, been found necessary to use a special purpose service to front end the directory to provide efficient access to the directory information when used for connection management.

6 Conclusion

The case studies presented in this report cover a reasonably broad spectrum of organisations, including computer suppliers, government organisations, universities and research institutes, as well as the UK and US defence community.

Over a hundred organisations were contacted, but only 15 felt that they were able to contribute to the study. Several of these projects were still in the early stages of pilot implementation, and from this one can conclude that X.500 is still a very new technology that, in general, is not yet embedded into many, particularly commercial, organisational operational IT systems. However, this situation could change rapidly over the next few years, as the existing pilot projects are rolled out into their respective organisations, and as other organisations start to adopt this new technology. Several of the pilot projects studied in phase 1 had become operational services a year later e.g. the SURFnet projects, and INESC. Other projects were already operational during the first study, e.g. NASA, Digital, Control Data, REDACS, Texas, MAFF and Adelaide. Several of the projects were hampered by the lack of products in the market place. Consequently many organisations had to build (and are still building) their own software tools and interfaces. The acceptance of X.500, and the success of future projects, should grow as more products come onto the market place in the coming years.

This report identifies some of the factors which were critical to the success of the X.500 projects studied. These were:

- 6.1 integration of directory access with other applications or communications services such as E-mail are essential if the vast majority of users are to frequently use the directory;
- 6.2 the establishment of organisational procedures, administrator commitment, and software tools for gathering and updating the data in the directory are essential but time consuming tasks, which are often underestimated;
- 6.3 senior management support for the deployment of an electronic directory is paramount.

Other issues which can have significance to the success (or otherwise) of the X.500 projects studied were: user involvement in the project, user interfaces, naming the entries in the DIT, technical problems, response times, security and legal issues. However, it must be remembered that since a majority of these projects were not initially intended for mission critical operational use by all users, (in other words, the directory was seen as being simply another nice service to have) some of these issues may become more critical once this is the case.

One thing that is evident, is that X.500 can be used in a wide variety of organisations all over the world, for a wide variety of purposes, and that X.500 would appear to have fulfilled its purpose of being an truly International Standard for directory services.

7 Acknowledgments

The author would like to thank CBC2 Division, DRA, Fort Halstead, Sevenoaks, Kent TN14 7BP for sponsoring this work under Contract No. MAL1a/0540, and John Ross of Security and Standards Consultancy Ltd for initiating the contract and contributing to the REDACS study.

The author would also like to thank all the contributors to the case studies, without whose input this research would not have been possible: Robert Anderson (Control Data Systems), Bertrand Buclin (Digital), Brian Gilmore (Edinburgh), Sylvain Langlois (EDF), Julia Brasse (EUNet), Chris Ridd (NHS), E Duarte (INESC), the late Richard Syrett (MAFF), Peter Yee (NASA), Amy Morris (COS), Piet Bovenga (Nijmegen), xx (Delft), Peter Jurg (SURFnet), Mark Prior (Adelaide), William Green (Texas), Bob Cooney (DoD), Paddy Boocock (REDACS).

Finally, the author would like to thank Thomas Lenggenhager of Switch and Nick Pope of Security and Standards Consultancy Ltd for help in devising the questionnaire.

8 Glossary of Terms

DSA Directory System Agent, the application that holds (part of) an organisations directory

database, and that `talks' the standard Directory protocol to other directory systems.

DUA Directory User Agent, the application that interfaces between the user and the Directory, by `talking' the standard Directory protocol.

LDAP Lightweight Directory Access Protocol, an Internet specification that simplifies the ISO/ITU-T access protocol.

MHS Message Handling Systems, systems that transfer electronic mail (such as X.400 systems)

NADF North American Directory Forum, an association of telecom organisations that are co-operating to define a public X.500 directory service

Quipu The first publicly available implementation of X.500

SMTP Simple Mail Transfer Protocol, the Internet standard for electronic mail

X.25 An International Standard for interconnecting computers in a network

X.400 An International Standard for electronic mail

X.500 An International Standard for directory services

9 References

[1] Getchell, A., Sataluri, S., "A Revised Catalog of Available X.500 Implementations", 1994, *Internet, RFC 1632*, May.

[2] Robbins, C.J. and Kille, S.E. (1991) *The ISO Development Environment: Users' Manual*, Volume 5: QUIPU, Version 7. July 18, available from UCL, London, via FTP or FTAM (file **isode-7-doc.tar.Z** in the directory **src/**).

[3] Rose, M.T. and Schoffstall, M.L. (1989) *An Introduction to a NYSErNet White Pages Pilot Project*. Dec.

[4] Directory Services: A Transition and Co-existence Approach. X.500 Integration Pilot Project. Phase II, Stage 1 Implementation Report, June 20 1994, Corporation for Open Systems International.

[5] Directory Services: A Transition and Co-existence Approach. X.500 Integration Pilot Project. Phase II, Stage 2 Implementation Report, September 28 1994, Corporation for Open Systems International.

[6] Directory Services: A Transition and Co-existence Approach. X.500 Integration Pilot Project. Phase II, Stage 3 Implementation Report, March 31 1995, Corporation for Open Systems International.

- [7] ITU-T Draft Recommendation X.rpmo: Procedures for Registration of International and Multinational Organisation Names, July 1994
- [8] Yeong, W., Howes, T. and Kille, S.E. (1993), "Lightweight Directory Access Protocol". *Internet, RFC 1487*, July.
- [9] Rose, M.T., Cass, D.E. (1987). "ISO Transport Services on top of the TCP: Version 3". *Internet, RFC 1006*, May
- [10] Paradise International Report May 1994, Available from University of London Computer Centre, 20 Guilford Street, London WC1N 2DZ.
- [11] Chadwick, D.W. "The Directory", Networks (Blackwell Scientific Publications), update 3, Feb 1989.
- [12] Chadwick, D.W. "Tutorial on X.500 - The Directory", pages T3-1 to T3-17, in Proceedings of the IFIP TCC 3rd Int Conf on Information Network and Data Communication, Lillehammer, Norway, March 1990
- [13] Chadwick, D.W., "X.500: 1988 v 1992", p23-29, in Proceedings of the Electronic Directories Conference, London, April 1991, Pinner:Blenheim Publications
- [14] Willmott, R., and Chadwick, D.W., "Technical Guide to the OSI Directory Service", NCC Blackwell, 1993, ISBN 1 85554 189 0
- [15] Chadwick, D.W., "Understanding X.500 (The Directory)", Chapman and Hall, June 1994, ISBN 0 412 43020 7
- [16] THE DIRECTORY. CCITT REC. X.500-X.521 (1988) | ISO/IEC STANDARD 9594:1990
- [16.1] X.500 | 9594.Part 1 Overview of Concepts, Models and Services
 - [16.2] X.501 | 9594.Part 2 Models
 - [16.3] X.511 | 9594.Part 3 Abstract Service Definition
 - [16.4] X.518 | 9594.Part 4 Procedures for Distributed Operations
 - [16.5] X.519 | 9594.Part 5 Protocol Specifications
 - [16.6] X.520 | 9594.Part 6 Selected Attribute Types
 - [16.7] X.521 | 9594.Part 7 Selected Object Classes
 - [16.8] X.509 | 9594.Part 8 Authentication Framework
- [17] THE DIRECTORY. CCITT REC. X.500-X.525 (1993) | ISO/IEC STANDARD 9594:1993
- [17.1-17.8] as per ref [16]
 - [17.9] X.525 | 9594.Part 9 Replication
- [18] Chadwick, D.W., "A Methodology for Conducting Case Studies and Surveys via the Internet", to be published.

Appendix 1 Questionnaire for Providers of the X.500 Service

1. Details of the Organisation

Organisation Name
Contact Address
Size of Organisation (No of Employees)
Geographical Spread of the Organisation
Brief Description of the Business
Current IT Infrastructure

2. X.500 Implementation - Project Definition Phase

Timescale
What was the original planned timescale for the project
Goals of project
What were the original goals of the project
Budget (Manpower, Equipment and Cash)
What were the original budgeted figures for the above
Project Champion/Sponsor
Was there an initial project sponsor/champion who was driving the project, and if so what was his/her position within the organisation. Did they have top management support?
User Involvement
Were the end users involved in the initial stages of defining the project?

3. Project Design Phase

Data Richness
What types of attribute are held in the directory e.g. telephone number, O/R Address, Fax number etc. Please list the main ones. Are there any unusual (i.e. non-standard) attribute types being used.
Schema
Which existing schema definitions were used, e.g. X.500 (88), X.500 (93), ISPs/EWOS, RFC 1274 (Cosine and Internet Schema), or manufacturer specific ones. What bespoke schema definitions had to be created specifically for this organisation. Who did this, the supplier or in-house expertise?
Entries
What types of object e.g. person, application, have entries in the directory, and what is the coverage in percentage terms e.g. 100% of employees, or all managers only.
Size
How many entries are to be in the organisation's DIT.

Names

How was the distinguished name of the organisation chosen. Did your organisation register its name with the appropriate body (e.g. DISC in the UK). How was the structure of the organisation's DIT subtree determined, and what is it (approximately). What procedure is used for allocating RDNs within the organisation.

Aliases

Do you make use of alias names, and if so, when and why.

Data protection

Did you have to contact the data protection registrar? Did you have to ask employees permission for their data to be included.

User Interfaces

Is the end-user a human or application or both.

Is the user interface an off-the-shelf product or has it been tailored specifically for your needs.

What functionality is given to end users.

Do you use an API, and if so which one.

Is the management interface off-the-shelf or bespoke.

Are either/both of the human interfaces pure X.500 interfaces, or are they integrated into those of other applications as well e.g X.400.

Distribution of DSAs and data

Do you have a centralised DSA or several DSAs.

If several, how many. Do they chain or refer requests to each other? Do they have a full set of references (cross, subordinate, superior) to each other.

Replication of data

If you have several DSAs, what data replication mechanism is used between them. Do DSAs and or DUAs cache data, and if so what 'cleaning' mechanism is used.

Synchronisation of data

How frequently is the data in X.500 updated from the other directories, databases and data sources. (Or is X.500 the master copy.)

Inter-organisational connectivity

Do you plan to connect your directory to any external ones. If so to which. Is this for access to external information or are external users allowed to access your organisation's information. Is there a part of your directory data that is externally accessible or inaccessible. What arrangements have you made for tariffing etc.

Security

How is the X.500 data protected? What sort of authentication (none, passwords or digital signatures) and access controls (none, standard or proprietary) are used. What validation must external people/applications present in order to access your directory information.

Protocols

Are pure ISO stacks used, or do you run over TCP/IP with RFC1006. How does the DUA connect to the DSA e.g. pure ISO, or LDAP.

4. Procurement Phase

For both DUAs and DSAs

Which makes of hardware were tested, and then chosen.

Which X.500 software were tested and chosen.

Interoperability testing

What assurances of interoperability were requested or carried out prior to procurement.

Integrated package

Was the X.500 system procured as part of a more general application system (e.g. as part of a messaging system).

5. Installation Phase

Training

What training was given to the technical and administrative staff on the project. (In this context administrative staff means directory administrators, who will be responsible for administering the directory database.)

Hardware installation

Was the installation performed by the supplier or in-house. Were any problems encountered in installing the hardware.

Software installation

Was the installation performed by the supplier or in-house. Were any problems encountered in installing the software. How long did it take (man days).

Configuration

Were there any problems in configuring the systems.

Data collection and loading

What are the sources of the X.500 data e.g. PBX, other electronic directories or databases.

What software tools were/are used for loading the database. Where did these originate from e.g. X.500 supplier or in-house.

X.500 interworking issues

Did all the components within the organisation interwork as expected, or were there any problems. Have you attempted to interconnect to an external organisation/implementation, and was this successful.

Integration with other applications

Did this work as expected. Did any modifications need to be made to the X.500 or other application software in order to integrate them together.

Bespoke tailoring.

Was any bespoke tailoring (either planned or unplanned) needed to the X.500 software in order for it to work as originally planned.

Bugs encountered

Were any bugs encountered in any of the software during installation or service introduction.

Non-conformance

Was any of the software non-conformant to the manufacturers specifications, or to what you were expecting. To the best of your knowledge, is any of the software non-conformant to the X.500 standard.

6. Service Introduction

Publicity

What publicity was given to users before/during the introduction of the service.

User Profiles

What are the profiles of the users of the X.500 system e.g. secretary, manager, technical expert etc.

User Training

How much training did you provide to the human users when introducing the service.

User Support

What level of support was needed initially by the users, and how does this compare to the current (operational) level.

User Feedback

What feedback have you had from the users about the service.

User Acceptance

Did the users readily accept the new technology, or was there a reluctance to use this new facility. What percentage of the initially targeted users actually used the service.

Did some try it and then revert to their old methods of working.

Usage Statistics

Were usage statistics kept. How many operations were made to X.500 per day.

7. Overall Project Management

Methodology

What project management methodology, if any, was used for the implementations.

User involvement

How much user involvement was there throughout the life of the implementation project. How much were their views considered.

Senior management involvement

Did senior management support the project throughout its lifetime, and were they kept informed of progress throughout.

Project team constituency

How many people were there in the project team, averaged throughout the life of the project. What was the maximum number of people at any one time.

Planning

Was the original project plan accurate, or did it have to be modified one or more times.

Control

How was progress monitored. Were there several intermediate milestones throughout the project.

Actual Timescale

What was the actual timescale for the implementation.

Actual Cost

What was the final cost.

Lessons

What were the major lessons learnt.

8. Operational Environment

Data Loading/Updates

Who is responsible for data updating, is it centralised or distributed to units within the organisation. Do users input their own data on line via directory protocols, or are only administrators allowed to. Is there a procedure for controlling updates.

Size

How many entries are currently in the organisation's DIT.

Synchronisation of data

Do you experience any problems in data synchronisation e.g. entries not being updated or deleted when they should be, or replication between different DSA systems.

Is X.500 data also held by other applications e.g. MSMail or X.400, and are there any problems in synchronising between these.

Support required

How much technical support is needed to ensure the smooth running of the systems (excluding system enhancements).

How much technical support is devoted to system enhancements.

How much administrative support is required to ensure that the data is kept current (if X.500 data is automatically downloaded from other systems, how much administrative support do these other systems require to keep their data current).

How much support is required for end users, be it help desk, training or whatever.

What sort of operational infrastructure is in place to support the system, coordinate updates, allocate RDNs etc.

Costs of ongoing maintenance and support

What are the total costs of the above, including hardware and software support.

Usage statistics

Are daily/weekly usage statistics kept, and if so what are they. What is the actual usage vs planned usage. Has the usage grown or shrunk since its introduction, and by how much.

Missing features

Are there any features missing from the current system that are:

- a) essential
- b) desirable
- c) nice to have

in order to provide a quality user service.

Success or Failure?

How would you rate the current service on a scale from 0 (Total Failure) to 10 (Unqualified Success).

9. Current/Future Developments

What additional features are planned to be added to the system, either now or in the future.

Please name the feature, state when it is planned to implement it, and how much it is expected to cost.